UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

NIK TURIK,	)	
	)	
Plaintiff,	)	No.
	)	
v.	)	JURY TRIAL DEMANDED
	)	
CARL'S GOLFLAND, INC.,	)	
	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Nik Turik, by and through his attorneys, Fegan Scott LLC, for his Complaint, alleges as follows:

I. INTRODUCTION

1. On August 29, 2019, Carl's Golfland announced that a breach in its online shopping website had occurred during the summer of 2019. While Defendant learned of the breach in late June 2019, it nonetheless failed to prevent the perpetrator from continuing to steal Defendant's online customers' personal information, including their credit card information (card number, expiration date, and CVV) as well as the first and last names, addresses, shipping information, emails and some phone numbers, well into July 2019.

2. Moreover, despite learning of the breach in late June 2019, Defendant failed to notify customers until two months later, during which time the perpetrators used Plaintiff's credit card information to make purchases.

3. Since the data breach occurred, Defendant's customers have been victims of credit card theft and sustained resulting economic loss. Plaintiff has and will incur costs to mitigate the risk, such as paying for "credit freezes" or credit monitoring products. Regardless of whether they have yet to incur out-of-pocket losses, all of the persons whose information was

stolen in the breach remain subject to a pervasive, substantial and imminent risk of identity theft and fraud.

4. This class action is brought on behalf of all natural persons victimized by the breach to redress the damage that they have suffered and to obtain appropriate equitable relief to mitigate the risk that Defendant will allow another breach in the future. Plaintiff and the nationwide class he seeks to represent assert claims for Defendant's negligence, negligence *per se*, violations of the Michigan Identity Theft Protection Act, and Michigan's Consumer Protection Act.

II. JURISDICTION

5. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, and Defendant is a citizen of a State different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

6. Venue is proper in this District under 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the claims occurred in the District.

III. PARTIES

7. Plaintiff Nik Turik is a resident and citizen of the State of Illinois (Cook County), and his Personal Information[1] was compromised in the Carl's Golfland data breach. Plaintiff received a notice on August 29, 2019 from Defendant that his Personal Information was

[1] As used throughout this Complaint, "Personal Information" is defined as all information exposed by the Carl's Golfland data breach, including all or any part or combination of name, address, birth date, driver's license information (any part of license number, state, home address, dates of issuance or expiration), telephone number, email address, tax identification number, credit card number, or other documents with personally identifying information (such as images of government-issued identifications).

compromised. As a direct result of the breach, Plaintiff's credit card information was used to make unauthorized purchases. Plaintiff has and will spend time and money purchasing credit freezes in order to mitigate possible harm. Plaintiff would not have purchased products from Defendant on-line had he known of Defendant's inadequate data security practices. In addition, as a result of the breach, Plaintiff Turik spent time and effort making multiple telephone calls to his bank and credit card company, monitoring his financial accounts, searching for fraudulent activity, and reviewing his credit report. Given the nature of the information stolen, Plaintiff remains at a substantial and imminent risk of future harm.

8. Defendant Carl's Golfland, Inc. is a Michigan corporation with its principal place of business located at 1976 S. Telegraph Rd., Bloomfield Hills, MI 48302.

IV. FACTS

9. According to Carl's Golfland, a breach in its online shopping website came to Defendant's attention through a bank inquiry in late June.

10. Defendant states that it completed a comprehensive forensics cyber audit of all of its systems. The audit report purportedly verifies that the perpetrator of the breach "obtained shopper credit card information (card number, expiration date, and CVV) as well as the first and last names, addresses, shipping information, emails and some phone numbers of our customers."

11. The breach occurred with customers who purchased with Defendant on-line between the dates of March 25 through July 14, 2019.

12. Defendant first learned of the vulnerability to its system in late June 2019. Yet Defendant waited until August 29, 2019 to publicly announce the breach in an email to customers. By waiting eight weeks after Defendant discovered the breach to notify customers, Defendant deprived consumers of the opportunity to take immediate precautionary measures to protect themselves from identity theft and fraud.

13. The breach has forced and will force consumers to spend money to protect themselves, including purchasing products such as credit monitoring and "credit freezes."

14. According to the FTC, a credit freeze, also known as a security freeze, allows a consumer to restrict access to their credit report, which in turn makes it more difficult for identity thieves to open new accounts in that consumer's name.

15. While credit freezes can be effective in thwarting fraudulent activity, they are also costly, time-consuming, and can create barriers for consumers who are quickly in need of credit.

16. For example, in order to institute a credit freeze, most consumers must pay a fee every time they want to freeze their credit, which can cost up to $10 per freeze depending on state law. If a consumer needs credit while under a credit freeze, she must first unfreeze her credit, again at a cost of up to $10 per unfreeze. The consumer then must pay again to have her credit frozen.

17. Because credit freezes are most effective when they are implemented with all three major credit reporting agencies ("CRAs"), consumers must pay Equifax, Experian, and TransUnion each time they want to freeze or unfreeze their credit. As Experian's website notes, "Those costs can add up."

18. Credit freezes can also be challenging to implement given that CRAs are notoriously difficult to contact. As noted by a New York Times commenter in the aftermath of the Equifax breach, "Some people are waiting until the middle of the night to try to use Equifax's security freeze website and even failing then to get through. It's like trying to get Bruce Springsteen tickets, except nobody wants to see this particular show."

19. Additionally, the lag time associated with freezing and unfreezing credit can create problems when a consumer quickly needs credit, which can make it difficult for

consumers to take out loans or make major purchases without planning days or weeks in advance. Experian's website acknowledges that, "Credit freezes can create delays and problems when credit is needed quickly in the case of applying for a loan, credit card, or even a job hunt. . . . During a freeze period, most companies will not extend credit until they check one's credit file with one or three major credit bureaus, and that takes time."

20. Although credit freezes are expensive and can be problematic for those seeking credit, they are among the best defenses to identity theft and fraud, and numerous consumer groups recommended that consumers freeze their credit in the aftermath of the breach.

21. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

22. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm

resulting from data breaches cannot necessarily rule out all future harm.

23. Defendant's actions and failures to act when required have caused Plaintiff and the Class defined below to suffer harm and/or face the significant and imminent risk of future harm, including:

a. theft of their Personal Information;

b. costs associated with requested credit freezes;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. costs associated with purchasing credit monitoring and identity theft protection services;

e. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach— including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised

accounts;

h. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being placed in the hands of criminals; and

i. continued risk of exposure to hackers and thieves of their Personal Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs and the Class.

24. Consequently, victims of the breach are at an imminent risk of fraud and identity theft for years to come.

V. CLASS ACTION ALLEGATIONS

25. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, Plaintiff seeks certification of the following nationwide class: "All natural persons residing in the United States whose Personal Information was compromised as a result of the data breach announced by Carl's Golfland on or about August 29, 2019, as identified by Carl's Golfland's records relating to that data breach."

26. ***Numerosity***: ***Federal Rule of Civil Procedure 23(a)(1).*** The members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. Plaintiff is informed and believes that the class may number in the thousands, making joinder impracticable. Those individuals' names and addresses are available from Defendant's records, and Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods.

27. ***Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3).*** This action involves common questions of law and fact, which predominate over

any questions affecting individual class members, including:

28. Whether Defendant knew or should have known that its computer systems were vulnerable to attack;

29. Whether Defendant failed to take adequate and reasonable measures to ensure its data systems were protected;

30. Whether Defendant failed to take available steps to prevent and stop the breach from happening;

31. Whether Defendant failed to disclose the material facts that it did not have adequate computer systems and security practices to safeguard consumers' Personal Information;

32. Whether Defendant failed to provide timely and adequate notice of the data breach;

33. Whether Defendant owed a duty to Plaintiff and Class members to protect their Personal Information and to provide timely and accurate notice of the data breach to Plaintiff and Class members;

34. Whether Defendant breached its duties to protect the Personal Information of Plaintiff and Class members by failing to provide adequate data security and by failing to provide timely and accurate notice to Plaintiff and Class members of the data breach;

35. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the unauthorized access and/or theft of consumers' Personal Information;

36. Whether Defendant's conduct amounted to violations of the Michigan state consumer protection act or data breach statute;

37. Whether Defendant's conduct amounted to violations of state consumer

protection statutes, and/or state data breach statutes;

38. Whether Defendant's conduct renders it liable for negligence, negligence per se, or unjust enrichment;

39. Whether, as a result of Defendant's conduct, Plaintiffs and Class members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled; and

40. Whether, as a result of Defendant's conduct, Plaintiffs and Class members are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief.

41. ***Typicality: Federal Rule of Civil Procedure 23(a)(3).*** Plaintiffs' claims are typical of other Class members' claims because Plaintiffs and Class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

42. Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4). Plaintiff is an adequate class representative because his interests do not conflict with the interests of Class members who he seeks to represent, Plaintiff has retained counsel competent and experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

43. The Class members' interests will be fairly and adequately protected by Plaintiff and his counsel.

44. ***Declaratory and Injunctive Relief: Federal Rule of Civil Procedure 23(b)(2).*** The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Defendant. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class members and

impair their interests. Defendant has acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

45. ***Superiority: Federal Rule of Civil Procedure 23(b)(3).*** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

VI. CHOICE OF LAW FOR NATIONWIDE CLAIMS

46. The State of Michigan has a significant interest in regulating the conduct of businesses operating within its borders. Michigan, which seeks to protect the rights and interests of Michigan and all residents and citizens of the United States against a company headquartered and doing business in Michigan, has a greater interest in the nationwide claims of Plaintiffs and Class members than any other state and is most intimately concerned with the claims and outcome of this litigation.

47. The principal place of business of Carl's Golfland, 1976 S. Telegraph Rd., Bloomfield Hills, MI 48302 is the "nerve center" of its business activities—the place where its high-level officers direct, control, and coordinate the corporation's activities, including its data security functions and major policy, financial, and legal decisions.

48. Defendant's response to the data breach at issue here, and corporate decisions surrounding such response, were made from and in Michigan.

49. Defendant's breaches of duty to Plaintiffs and Class members emanated from Michigan.

50. On Carl's Golfland's website on which Plaintiff and Class members made purchases, it publishes terms and conditions, which provide: "This site is created and controlled by Carl's Golfland Inc. in the state of Michigan, USA. As such, the laws of the state Michigan will govern these disclaimers, terms and conditions, without giving effect to any principles of conflict of laws."

51. Application of Michigan law to the Class with respect to Plaintiffs' and Class members' claims is neither arbitrary nor fundamentally unfair because Michigan has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiff and the Class.

CAUSES OF ACTION

COUNT I
MICHIGAN IDENTITY THEFT PROTECTION ACT, MICH. COMP. LAWS ANN. §§ 445.72, ET SEQ.

52. Plaintiff incorporates the foregoing allegations as if fully alleged herein.

53. Defendant is a business that owns or licenses computerized data that includes Personal Information as defined by Mich. Comp. Laws Ann. § 445.72(1).

54. Plaintiff's and Class members' Personal Information, as covered under Mich. Comp. Laws Ann. § 445.72(1), was subject to a data breach.

55. Defendant is required to accurately notify Plaintiff and Class members if it discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), without

unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

56. Because Defendant discovered a security breach and had notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), Defendant had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

57. By failing to disclose the data breach in a timely and accurate manner, Defendant violated Mich. Comp. Laws Ann. § 445.72(4).

58. As a direct and proximate result of Defendant's violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiff and Class members suffered damages, as described above.

59. Plaintiff and Class members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including a civil fine.

COUNT II
MICHIGAN CONSUMER PROTECTION ACT,
MICH. COMP. LAWS ANN. §§ 445.903, ET SEQ.

60. Plaintiff realleges and incorporates the foregoing allegations as though fully set forth herein.

61. Plaintiff, Class members and Defendant are "persons" as defined by Mich. Comp. Laws Ann. § 445.903(d).

62. Defendant advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

63. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

64. Representing that its goods and services have characteristics, uses, and benefits that they do not have, in violation of Mich. Comp. Laws Ann. § 445.903(1)(c);

65. Representing that its goods and services are of a particular standard or quality if they are of another in violation of Mich. Comp. Laws Ann. § 445.903(1)(e);

66. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb); and

67. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter, in violation of Mich. Comp. Laws Ann. § 445.903(1)(cc).

68. Defendant's unfair, unconscionable, and deceptive practices include:

69. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class members' Personal Information, which was a direct and proximate cause of the data breach;

70. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security, which was a direct and proximate cause of the data breach;

71. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' Personal Information;

72. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Class members' Personal Information; and

73. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' Personal Information.

74. Defendant's representations and omissions were material because they were likely

to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of consumers' Personal Information.

75. Defendant intended to mislead Plaintiff and Michigan Subclass members and induce them to rely on its misrepresentations and omissions.

76. Defendant acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiff and Class members' rights.

77. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

78. Plaintiff and Class members seek all monetary and nonmonetary relief allowed by law, including the greater of actual damages or $250, injunctive relief, and any other relief that is just and proper.

COUNT III
NEGLIGENCE

79. Plaintiff realleges and incorporates the foregoing allegations as if fully set forth herein.

80. Defendant owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their Personal Information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing its security systems to ensure that Plaintiffs' and Class members'

Personal Information in its possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

81. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

82. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiffs and Class Members would be harmed by the failure to protect their Personal Information because hackers routinely attempt to steal such information and use it for nefarious purposes, Defendant knew that it was more likely than not Plaintiffs and other Class members would be harmed.

83. Defendant's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Personal Information by companies such as Defendant. Various FTC publications and data security breach orders further form the basis of Defendant's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

84. Timely notification was required, appropriate and necessary so that, among other things, Plaintiffs and Class members could take appropriate measures to freeze or lock their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change

usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Defendant's misconduct.

85. Defendant breached the duties it owed to Plaintiff and Class members described above and thus was negligent. Defendant breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the Personal Information of Plaintiff and Class members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose that Plaintiffs' and the Class members' Personal Information in Defendant's possession had been or was reasonably believed to have been, stolen or compromised.

86. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class members, their Personal Information would not have been compromised.

87. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial. Plaintiffs' and Class members' injuries include:

a. theft of their Personal Information;

b. costs associated with requested credit freezes;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. costs associated with purchasing credit monitoring and identity theft protection services;

e. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach— including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

h. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being placed in the hands of criminals; and

i. continued risk of exposure to hackers and thieves of their Personal Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff and Class members.

COUNT IV
NEGLIGENCE PER SE

88. Plaintiff realleges and incorporates the foregoing allegations as if fully set forth

herein.

89. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by companies such as Defendant of failing to use reasonable measures to protect Personal Information. Various FTC publications and orders also form the basis of Defendant's duty.

90. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Personal Information and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored and the foreseeable consequences of a data breach.

91. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

92. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

93. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and the Class.

94. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

WHEREFORE, Plaintiff respectfully requests that:

a. The Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiff's Counsel as Class Counsel;

b. The Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

c. The Court award Plaintiff and Class members compensatory, consequential, general, and nominal damages in an amount to be determined at trial;

d. The Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

e. Plaintiffs be granted the declaratory relief sought herein;

f. The Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

g. The Court award pre- and post-judgment interest at the maximum legal rate; and The Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial on all claims so triable.

Dated: August 30, 2019

FEGAN SCOTT LLC

By: /s/ Timothy A. Scott
Elizabeth A. Fegan
Timothy A. Scott
FEGAN SCOTT LLC
150 S. Wacker Dr., 24th Floor
Chicago, IL 60606
Ph: 312.741.1019
Fax: 312.264.0100
beth@feganscott.com
tim@feganscott.com

David Freydin
Law Offices of David Freydin Ltd.
8707 Skokie Blvd, Suite 305
Skokie, IL 60077
(847) 972-6157
david.freydin@freydinlaw.com

Counsel for Plaintiff